REMARKS

Claims 1-14 were pending in the present application. Claims 1-14 have been rejected. New claims 15-18 have been added. It is respectfully submitted that no new matter has been added. Upon entry of the current amendments, claims 1-18 will be pending. Reconsideration of the Office Action dated July 13, 2007 is respectfully requested in view of the above amendments and following remarks.

Claim Rejections Under 35 U.S.C. §102(b):

Claims 1, 5, 7, 8, 12, and 14 are rejected under 35 U.S.C. 102(b) as allegedly being anticipated by U.S. Patent No. 7,162,635 (Bisbee et al.). The Examiner asserted that Bisbee et al. provides a method substantially as recited in these claims. Reconsideration of this rejection is requested in view of the following remarks.

Bisbee et al. disclose a systems and methods for providing a verifiable chain of evidence and security for the transfer and retrieval of documents and other information objects in digital formats. (Bisbee et al. at col. 1, lns. 20-24). The tokens disclosed by Bisbee et al. are security tokens and are not session tokens, which is the type of token recited in the pending claims of the present application.

A security token (also known as a hardware token, authentication token or cryptographic token) is a physical device that an authorized user of computer services is given to aid in authentication. (See, e.g., http://en.wikipedia.org/wiki/Token). Security or hardware tokens are physical devices that are typically small enough to be carried in a pocket or purse and often are designed to attach to the user's keychain. Some may store cryptographic keys, such as a digital signature, or biometric data, such as a fingerprint. This is exactly the type of token disclosed by Bisbee et al.

For example, Bisbee et al. describes the public/private key is advantageously delivered in the form of **a Token such as an electronic circuit card** conforming to the standards of the PC Memory Card Interface Association (a PCMCIA card or PC Card) for use in the originator's computer. Further the Token disclosed by Bisbee et al. is defined as a portable transfer device that is used for transporting keys, or parts of keys. It will be understood that PC Cards are just one form of delivery mechanism for public/private keys;

other kinds of Tokens may also be used, such as floppy diskettes, Smart Cards, universal serial bus (USB) tokens, integrated circuits, etc. All of these Tokens are physical devices used for security purposes. Moreover, Bisbee et al. state that using an integrated circuit, such as a memory device or a programmable processor with memory, for a Token has the advantage of small size, enabling Tokens to be included in many communication and computing devices, like cellular telephones, personal digital assistants, handheld computers, identification badges, etc. (Bisbee et al. at col. 10, lns. 6-25 and col. 11, lns. 20-32). In addition, Bisbee et al. do not disclose or teach enabling or disabling a functionality of a browser based on a token communicated from a server to a browser.

In contrast, the claimed subject matter comprises a session token which is a unique identifier which may be generated and sent from a server to a software client to identify an interaction session and which the client usually stores as an HTTP cookie. (See, e.g., http://en.wikipedia.org/wiki/Token). In computer science, in particular networking, a session is either a lasting connection using the session layer of a network protocol or a lasting connection between a user (or user agent) and a peer, typically a server, usually involving the exchange of many packets between the user's computer and the server. A session is typically implemented as a layer in a network protocol (e.g., telnet or FTP).

In the case of transport protocols which do not implement a formal session layer (e.g., UDP) or where sessions at the session layer are generally very short-lived (e.g., HTTP), sessions may be maintained by a higher level program using a method defined in the data being exchanged. For example, an HTTP exchange between a browser and a remote host may include an HTTP cookie which identifies state, such as a unique session ID, information about the user's preferences or authorization level.

According to embodiments of the present invention, a token is communicated from the server 200 to the browser 214 or viewer 213 after a document is requested. The token is preferably a text string embedded in the HTML or HTTP response headers, and is preferably a hash or digital signature of the web site's domain name and/or other information. When the browser 214 receives this token, it is decrypted and based on the results, certain browser functionality is enabled or disabled. Such functionalities include, but are not limited to, pop-up ads, video and/or audio content, plug-ins, controls, etc. By using a token in accordance with the present invention, content providers/vendors are able to control what features are

present in the browser, as well as the content that may be displayed by the browser. These features enable control over media distribution to prevent unauthorized or illegal use of content. Thus, after contacting the web site 200, the web browser 214 or viewer 213 may render the HTML/XML code in the document 204 and displays the document and related graphical content with the functionalities enabled by the token.

The independent claims recite use of a session type token to enable or disable functionality of a browser. Independent claim 1 is representative and recites, in part:

> receiving a response from the server, the response containing a token;
> interpreting information contained in said token; and
> invoking a level of functionality in said application program in accordance with said token.

Independent claim 8 recites similar features. It is respectfully submitted that the above recited claim features are not disclosed or taught by Bisbee et al., or any of the other cited references. Accordingly, withdrawal of the rejection of the independent claims 1 and 8 under 35 U.S.C. §102(e) is requested.

A dependent claim includes all of the limitations of the base claim and any intervening claims and therefore a dependent claim can not be anticipated if the claim from which it depends is not anticipated. As such, applicant respectfully submits that claims 5 and 7 which depend, either directly or indirectly, from independent claim 1; and claims 12 and 14 which depend, either directly or indirectly, from independent claim 8 are also not anticipated by Bisbee et al. for the reason provided above with respect to independent claims 1 and 8. Accordingly, withdrawal of the rejection of these dependent claims is also requested.

Further with respect to claims 5 and 12, while Bisbee et al. may disclose a digital certificate (see e.g., Bisbee et al. at col. 11, lns. 21-38), it does not disclose a token comprising a digital certificate. As explained above, the only token disclosed by Bisbee et al. is a physical device, such as a electronic circuit card (see Bisbee et al. at col. 10, lns. 6-17). Accordingly, withdrawal of the rejection of claims 5 and 12 over the Bisbee et al. reference is solicited for this additional reason.

With respect to claims 7 and 14, a browser may be disclosed by Bisbee et al. however invoking a level of functionality in a browser control to invoke a viewer, as recited in claims 7 and 14, is not disclosed. Accordingly, withdrawal of the rejection of claims 7 and 14 over the Bisbee et al. reference is requested for this additional reason.

Claim Rejections Under 35 U.S.C. §103(a):

Claims 2-4, 6, 9-11 and 13 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Bisbee et al. as applied to claim 1 above, and further in view of the examiner taking official notice. Reconsideration of this rejection is requested in view of the above remarks and the following remarks.

To establish prima facie obviousness under 35 U.S.C. 103(a), MPEP §2142 first requires the prior art references when combined must teach or suggest all the claim limitations. Second, there must be a reasonable expectation of success. Finally, some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Applicants' disclosure.

The Examiner asserted that, although Bisbee et al. do not specifically disclose the recited limitations of the claims, the examiner takes official notice that these elements are well known in the art of security systems. (see Office Action at page 3). Applicant respectfully traverses these rejections as follows.

As discussed above with respect to the claim rejections under 35 U.S.C. §102(b), Bisbee et al. fail to disclose all of the features of the independent claims. Further Bisbee et al, fails to teach or suggest the above noted features. Since claims 2-4, 6, 9-11, and 13 all depend, either directly or indirectly, from independent claims 1 and 8, these dependent claims include all of the limitations of the claim(s) from which they depend and are allowable for the reasons stated above. Accordingly, withdrawal of the claims rejections under 35 U.S.C. §103(a) is solicited.

New claims 15-18 have been added. Support for these claims can be found, for example, in the specification at paragraphs 0028 and 0029. Bisbee et al. and the other cited references do not disclose or teach the features of these new claims. For example, new independent claim 15 recites:

> A method for content providers to control features that are presented in a browser, said method comprising:
> providing a token to a web site;
> associating said token with said web site;
> receiving at said web server a request for information for a web site from a browser;
> invoking a level of functionality of said web site at said browser based on a presence or absence of said token.

These features are not disclosed or taught by the cited references. Further, new claim 16 recites that invoking a level of functionality of said web site at said browser further comprises: invoking a full level of functionality of said web site at said browser for web sites having one of said tokens; and invoking a reduced level of functionality of said web site at said browser for web sites not having one of said tokens. These features are also not disclosed or taught by the cited art.

Conclusion:

In view of the foregoing amendments and remarks, applicant submits that the above-identified application is in condition for allowance. Early notification to this effect is respectfully requested. If the Examiner has any questions regarding this response, the Examiner is invited to contact the undersigned attorney at (215) 568-3100.

Date: November 6, 2007

/Michael K. Jones/
Michael K. Jones
Registration No. 41,100

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439